UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

IN RE WASHINGTON COLLEGE DATA SECURITY INCIDENT LITIGATION	Case No. 1:23-cv-03258-RDB (Lead Action)

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Abigail Collins, Taylor Breshanan, Caitlyn Creasy, and Vincent Pacheco ("Plaintiffs") bring this Class Action Petition ("Petition") against Defendant Washington College ("WC" or "Defendant"), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this action against WC for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including, but not limited to: full names and Social Security numbers (collectively, "personally identifiable information" or "PII").

2. On March 14, 2023, Defendant "became aware of suspicious activity on [its] network and servers."[1] In response, Defendant "launched an investigation in consultation with an external team of cybersecurity professionals who regularly investigate and analyze these types of situations to determine whether any sensitive data had been compromised as a result of the incident."[2] As a result of that investigation, Defendant concluded—on October 20, 2023—that "an

[1] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/a40bead5-bfc4-4455-940e-7837658c9d6c.shtml

[2] *Id.*

unauthorized actor accessed [its] systems between February 11, 2023 and March 14, 2023, and as a result, likely obtained certain files containing some of [Plaintiffs' and Class Members'] personal information."[3]

3. Defendant's investigation concluded that the PII compromised in the Data Breach included Plaintiffs' and approximately 13,168 other individuals' information.[4]

4. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence, at a minimum, and violates federal and state statutes.

5. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct, including (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long

[3] *Id.*

[4] According to the report submitted to the Office of the Maine Attorney General, 13,168 individuals were impacted. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/a40bead5-bfc4-4455-940e-7837658c9d6c.shtml

as Defendant fails to undertake appropriate and adequate measures to protect the PII.

6. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party.

7. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to damages and injunctive and other equitable relief.

PARTIES

8. Plaintiff Abigail Collins is an adult individual and, at all relevant times herein, a resident and citizen of Maryland, residing in Worton, Maryland.

9. Plaintiff, Taylor Bresnahan, is natural person and citizen of Maryland. He resides in Arnold, Maryland where he intends to remain.

10. Plaintiff Caitlyn Creasy is a natural person, resident, and a citizen of Parkville, Maryland.

11. Plaintiff Vincent Pacheco is a natural person, resident, and a citizen of Parkville, Maryland.

12. Defendant Washington College is a corporation organized under the state laws of Maryland, with its principal place of business located in Chestertown, Maryland.

JURISDICTION AND VENUE

13. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, as defined below, is a citizen of a different state than Defendant,[5] there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

14. This Court has general personal jurisdiction over Defendant because it maintains its principal place of business in this District, regularly conducts business in Maryland, and has sufficient minimum contacts in Maryland.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Defendant's Business

16. Defendant is a Maryland-based college that currently enrolls "roughly 1,400 students[.]"[6]

17. Plaintiffs and Class Members are or were students and/or student applicants at WC or provided Defendant with the relevant PII for some other purpose (*e.g.,* employment or application for employment or study).

18. To enroll in classes or other programs at Defendant, Plaintiffs and Class Members were required to provide sensitive and confidential PII, including but not limited to: their names

[5] According to the report submitted to the Office of the Maine Attorney General, 44 Maine residents were impacted in the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/a40bead5-bfc4-4455-940e-7837658c9d6c.shtml

[6] https://www.washcoll.edu/about/index.php

and Social Security numbers. The same or similar information was provided by other victims of this Data Breach, including employees of Defendant or applicants for employment or admission.

19. In collecting and maintaining the PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class members themselves took reasonable steps to secure their PII.

20. Under state and federal law, businesses like Defendant have duties to protect its current and former employees and students' PII and to notify them about breaches.

21. Upon information and belief, Defendant made promises and representations to its students and employees, including Plaintiffs and Class Members, that the PII collected from them as a condition of enrollment and/or their employment would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

22. Indeed, Defendant's Privacy Policy provides that:

> We respect your privacy
>
> Any and all information collected on this site will not be sold, rented, disclosed or loaned. Your information will be held with the utmost care and will not be used for anything other than official business.[7]

23. Via its "Mandated Federal Policies," Defendant promises that: "Washington College students are granted an automatic expectation of privacy for their education records."[8]

24. Again, via its "Confidentiality Agreement," Defendant declares that:

---

[7] https://www.washcoll.edu/privacy-policy/index.php

[8] *Mandated Federal Policies*, WASHINGTON COLLEGE, https://www.washcoll.edu/people_departments/offices/student-affairs/student-handbook/mandated-federal-policies/index.php/ (last visited Dec. 4, 2023).

a. "disclosure . . . is prohibited" of "educational, financial, and employment records that contain individually identifiable information;"[9]

b. "Information on individuals, other than published information, is not to be shared with individuals anywhere outside of the office;"[10]

c. "accessing, releasing, or using information without authorization that Washington College considers privileged or confidential violates College policy."[11]

25. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

26. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

27. Defendant had obligations created by contract, industry standards, federal, state, and common law, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

28. Plaintiffs and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach

29. On or about November 15, 2023, Defendant began sending Plaintiffs and other victims of the Data Breach an untitled letter (the "Notice Letter") informing them that a Data

[9] *Confidentiality Agreement*, WASHINGTON COLLEGE, https://www.washcoll.edu/people_departments/offices/human-resources/files/confidentiality-agreementpdf.pdf/ (last visited Dec. 4, 2023).
[10] *Id*.
[11] *Id*.

Breach occurred that impacted files contained Plaintiffs' full name and Social Security number.

30. Omitted from the Notice Letter the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. Defendant also waited until November 15, 2023, before it began notifying the class—a full 246 days after Defendant became aware of its own Data Breach.

31. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

32. When Defendant did notify Plaintiffs and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class:

a. "we recommend that you place an initial one (1) year 'Fraud Alert' on your credit files;"

b. "request a 'Security Freeze' be placed on your credit file;"

c. "Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies;" and

d. "contact law enforcement, such as the [] Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft."[12]

33. Despite providing minimal details about the breach, the Notice Letter shows that from February 11, 2023, until March 14, 2023, Defendant was hacked.[13] But Defendant only

[12] *Id*.
[13] *Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/a40bead5-bfc4-4455-940e-7837658c9d6c.shtml (last visited Dec. 4, 2023).

noticed its own Data Breach on March 14, 2023—a full *31 days after* the Data Breach began.[14]

34. Worryingly, Defendant has described this Data Breach as a "ransomware incident."[15]

35. Worse yet, Defendant has admitted that "an unauthorized actor *gained access* to Washington College's systems, via VPN."[16] And thus, the cybercriminals "likely obtained certain files."[17]

36. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted PII of Plaintiffs and Class Members, including their names, Social Security numbers, passport numbers, government ID numbers, and driver's license numbers.. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach.

37. Defendant injured at least 13,168 persons—via the exposure of their PII—in the Data Breach.[18] Upon information and belief, these 13,168 persons include Defendant's current and former employees and students.

38. Since the breach, Defendant has promised to "evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information."[19] But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

39. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

40. Further, the Notice of Data Breach shows that Defendant cannot—or will not—

[14] *Id*.
[15] *Id*.
[16] *Id*. (emphasis added).
[17] *Id*.
[18] *Id*.
[19] *Id*.

determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when.

41. Because of Defendant's Data Breach, the sensitive PII of Plaintiffs and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class members.

42. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) gained actual access to sensitive data via VPN, and (3) engaged in a "ransomware" hack.[20]

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

43. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII is used;

b. diminution in value of their PII;

c. compromise and continuing publication of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII; and

[20] *Id*.

h. continued risk to their PII—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

44. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

45. The value of Plaintiffs and Class's PII on the black market is considerable. Stolen PII trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

46. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

47. One way that criminals profit from stolen PII is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

48. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

49. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class members, and it is reasonable for any trier of fact, including this

Court or a jury, to find that Plaintiffs and other Class members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

50. Defendant disclosed the PII of Plaintiffs and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

51. Defendant's failure to promptly and properly notify Plaintiffs and Class members of the Data Breach exacerbated Plaintiffs and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

52. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

53. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[21]

54. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack.

55. Therefore, the increase in such attacks, and attendant risk of future attacks, was

[21] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

56. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

57. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[22] The FTC declared that, *inter alia*, businesses must: (a) protect the personal customer information that they keep; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems.

58. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

59. Furthermore, the FTC explains that companies must: (a) not maintain information longer than is needed to authorize a transaction; (b) limit access to sensitive data; (c) require complex passwords to be used on networks; (d) use industry-tested methods for security; (e) monitor for suspicious activity on the network; and (f) verify that third-party service providers use reasonable security measures.

60. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an

[22] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

61. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former employees and students' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

62. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

63. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

64. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

PLAINTIFFS' EXPERIENCES

Plaintiff Abigail Collins

65. Plaintiff Abigail Collins is a student of Washington College and a victim of the Data Breach.

66. Plaintiff Collins's information was stored with Defendant as a result of her dealings with Defendant.

67. As required in order to obtain services from Defendant, Plaintiff Collins provided Defendant with highly sensitive personal information, who then possessed and controlled it.

68. As a result, Plaintiff Collin's information was among the data accessed by an unauthorized third-party in the Data Breach.

69. Plaintiff Collins received a letter from Defendant, dated November 15, 2023, stating that their PII was involved in the Data Breach (the "Notice").

70. Plaintiff Collins was unaware of the scale of the Data Breach until she received that letter. Although she was aware a cybersecurity incident occurred in March due to the inaccessibility of school technology during that time, she was not aware that her PII might be involved until she received the letter.

71. As a result, Plaintiff Collins was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring their accounts with heightened scrutiny and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

72. Plaintiff Collins was also injured by the material risk to future harm they suffer

based on Defendant's breach; this risk is imminent and substantial because Plaintiff's data has been exposed in the breach, the data involved, including Social Security numbers, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendant's clientele, that some of the Class's information that has been exposed has already been misused.

73. Plaintiff Collins suffered actual injury in the form of damages to and diminution in the value of their PII—a condition of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

74. Plaintiff Collins, as a result of the Data Breach, has increased anxiety for their loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling their PII.

75. Plaintiff Collins has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII, in combination with their name, being placed in the hands of unauthorized third parties/criminals.

76. Plaintiff Collins has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Taylor Bresnahan

77. Plaintiff Taylor Bresnahan is a former student of Defendant (having graduated in 2013).

78. Defendant obtained and maintained Plaintiff Bresnahan's PII.

79. As a result, Plaintiff was injured by Defendant Bresnahan's Data Breach.

80. As a condition of being a student of Defendant, Plaintiff Bresnahan provided Defendant with his PII. Defendant used that PII to facilitate its provision of educational services to Plaintiff Bresnahan, including to obtain payment for its educational services.

81. Plaintiff Bresnahan provided his PII to Defendant and trusted WC would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Bresnahan's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

82. Plaintiff Bresnahan reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII.

83. Plaintiff Bresnahan does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

84. Plaintiff Bresnahan received a Notice of Data Breach dated November 15, 2023.

85. On information and belief, Plaintiff Bresnahan's PII has already been published—or will be published imminently—by cybercriminals on the dark web.

86. Through its Data Breach, Defendant compromised Plaintiff Bresnahan's full name and Social Security number.

87. Plaintiff Bresnahan has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff Bresnahan to take those steps in its breach notice.

88. Plaintiff Bresnahan fears for his personal financial security and worries about what information was exposed in the Data Breach.

89. Because of Defendant's Data Breach, Plaintiff Bresnahan has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

90. Plaintiff Bresnahan suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

91. Plaintiff Bresnahan suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

92. Plaintiff Bresnahan suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

93. Because of the Data Breach, Plaintiff Bresnahan anticipates spending considerable amounts of time and money to try and mitigate his injuries.

94. Today, Plaintiff Bresnahan has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Caitlyn Creasy

95. Plaintiff Creasy is a former WC student and employee, who attended and worked at WC from approximately 2016 through 2020.

96. In order to enroll at WC and/or as a condition of her employment at WC, she was required to provide her PII to Defendant, including her name and Social Security number.

97. At the time of the Data Breach–February 11, 2023 through March 14, 2023–Defendant retained Plaintiff's PII in its system, despite no longer being a student or employee at WC for approximately 3 years.

98. Plaintiff Creasy is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted

unencrypted sensitive PII over the internet or any other unsecured source.

99. Plaintiff Creasy received the Notice Letter, by U.S. mail, directly from Defendant, dated November 15, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her full name and Social Security number.

100. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Creasy made reasonable efforts to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, signing up for the credit monitoring and identity theft protection services offered by Defendant, and monitoring her credit for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

101. Plaintiff Creasy suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

102. Plaintiff Creasy additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

103. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

104. As a result of the Data Breach, Plaintiff Creasy is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

105. Plaintiff Creasy has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Vincent Pacheco

106. Plaintiff Pacheco is a former WC student and employee, who attended WC from approximately 2017 through 2021 and worked at WC from approximately 2019 to 2021.

107. In order to enroll at WC and/or as a condition of his employment at WC, he was required to provide his PII to Defendant, including his name and Social Security number.

108. At the time of the Data Breach—February 11, 2023 through March 14, 2023—Defendant retained Plaintiff's PII in its system, despite no longer being a student or employee at WC for approximately 2 years.

109. Plaintiff Pacheco is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

110. Plaintiff Pacheco received the Notice Letter, by U.S. mail, directly from Defendant, dated November 15, 2023. According to the Notice Letter, Plaintiff's PII was

improperly accessed and obtained by unauthorized third parties, including his full name and Social Security number.

111. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter as well as signing up for the credit monitoring and identity theft protection services offered by Defendant. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

112. Plaintiff Pacheco suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

113. Plaintiff Pacheco additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

114. Plaintiff Pacheco anticipates spending considerable time and money on an

ongoing basis to try to mitigate and address harms caused by the Data Breach.

115. As a result of the Data Breach, Plaintiff Pacheco is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

116. Plaintiff Pacheco has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

117. Plaintiffs bring this action on behalf of themselves and all other persons similarly situated.

118. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

> **Nationwide Class**
> All persons in the United States whose PII was compromised as a result of the Data Breach, for which Defendant provided notice in November 2023 (the "Class").
>
> **Maryland Subclass**
> All persons in the state of Maryland whose PII was compromised as a result of the Data Breach, for which Defendant provided notice in November 2023 (the "Maryland Subclass").

119. Excluded from the Classes are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and members of their staff.

120. The proposed Classes meet the criteria for certification.

121. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. At least 13,168 individuals were notified by Defendant of the Data Breach,

according to the breach report submitted to Maine's Attorney General's Office.[23] The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

122. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations and industry standards;

d. Whether Defendant owed a duty to Class Members to safeguard their PII;

e. Whether Defendant breached its duty to Class Members to safeguard their PII;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

h. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

i. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

123. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class member, was compromised in the Data Breach.

[23] https://apps.web.maine.gov/online/aeviewer/ME/40/a40bead5-bfc4-4455-940e-7837658c9d6c.shtml

124. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

125. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

126. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

127. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

128. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII; and

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts.

FIRST COUNT
Negligence
(On Behalf of Plaintiffs and the Class)

129. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

130. Defendant required Plaintiffs and Class Members to submit sensitive, non-public, personal information in order to enroll in one of Defendant's classes or programs or be eligible for employment.

131. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and the individuals that entrusted their PII to Defendant.

132. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to design, implement, and monitor systems, policies, and processes by which it could reasonably prevent and detect a breach of their security systems in

a reasonably expeditious period of time.

133. Defendant had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

134. Defendant owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with industry standards concerning data security would result in the compromise of that PII —just like the Data Breach that ultimately came to pass.

135. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

136. Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

137. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

138. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII . The specific negligent acts and omissions

committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to detect in a timely manner that Class Members' PII had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

139. The breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches generally and in the higher education industry.

140. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

141. Plaintiffs and the putative class members had no way to protect themselves from the damage Defendant is responsible for.

142. The imposition of a duty of care on Defendant to safeguard the PII it maintained is appropriate because any social utility of Defendant's conduct—of which little, if any, exists––is outweighed by the injuries suffered by Plaintiffs and Class Members as a result of the Data Breach.

143. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and unsecure manner.

144. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

145. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

146. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Breach Of Implied Contract
(On Behalf of Plaintiffs and the Class)

147. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

148. When Plaintiffs and Class Members provided their PII to Defendant in exchange for enrolling in classes, applying for enrollment, or obtaining employment at Defendant, they

entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information and to destroy any PII that it was no longer required to maintain.

149. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

150. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

151. In accepting the PII of Plaintiffs and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

152. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including the FTC Act, and were consistent with industry standards.

153. Plaintiffs and Class Members paid money and/or provided their labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

154. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

155. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

156. Plaintiffs and Class Members fully and adequately performed their obligations

under the implied contracts with Defendant.

157. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII or to destroy it once it was no longer necessary to retain the PII.

158. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

159. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

160. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD COUNT
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

161. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

162. Given the relationship between Defendant and Plaintiffs and Class members, where Defendant became guardian of Plaintiffs' and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiffs and Class members, (1) for the safeguarding of Plaintiffs and Class members' PII; (2) to timely notify Plaintiffs and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

163. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of Defendant's relationship with them—especially to

secure their PII.

164. Because of the highly sensitive nature of the PII, Plaintiffs and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

165. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class members' PII.

166. Defendant also breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

167. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

FOURTH COUNT
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

168. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

169. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

170. Defendant owed a duty to its current and former employees and students, including Plaintiffs and the Class, to keep this information confidential.

171. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class members' PII is highly offensive to a reasonable person.

172. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

173. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

174. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

175. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

176. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

177. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

178. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the dark web.

179. Unless and until enjoined and restrained by order of this Court, Defendant's

wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

180. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class.

181. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FIFTH COUNT
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

182. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

183. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and Class Members.

184. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

185. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their PII and paid money and/or provided labor to Defendant and/or

its agents in connection with their admission applications and/or employment at Defendant, and in so doing, provided Defendant with their PII based on the understanding that the benefits derived therefrom would, in part, be used to fund adequate data security. In exchange, Plaintiffs and Class Members should have received from Defendant the educational services, and/or employment position that were the subject of the transaction and have their PII protected with adequate data security.

186. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

187. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and instead directed those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

188. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

189. Defendant failed to secure Plaintiffs' and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

190. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

191. Defendant obtained a benefit from Plaintiffs and Class Members by fraud and/or

the taking of an undue advantage, in that it misrepresented and omitted material information concerning its data security practices when Plaintiffs and Class Members relied upon it to safeguard their PII against foreseeable risks.

192. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant or obtained educational services and/or employment at Defendant.

193. Plaintiffs and Class Members have no adequate remedy at law.

194. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (xx) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

195. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injuries and/or harms.

196. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs

and Class Members overpaid for Defendant's services.

SIXTH COUNT
Violations of Maryland's Consumer Protection Act & The Maryland Personal Information Act
(On Behalf of Plaintiffs and the Maryland Subclass)

197. Plaintiffs re-allege and incorporate the above allegations, as if fully set forth herein, and bring this claim on behalf of themselves and the Maryland Subclass (the "Class" for the purposes of this count).

198. This cause of action is brought pursuant to the Maryland Consumer Protection Act, § 13-101, *et seq.* and the Maryland Personal Information Protection Act, § 14-3501, *et seq.*

199. The purpose of the Maryland Consumer Protection Act is "to set certain minimum statewide standards for the protection of consumers across the State [of] [Maryland]."

200. The Maryland Personal Information Protection Act was implemented to, among other things, "[t]o protect personal information from unauthorized access, use, modification, or disclosure...of an individual residing in the State [of] [Maryland]."

201. A violation of the Maryland Personal Information Protection Act "is an unfair or deceptive trade practice."

202. Defendant has violated the Maryland Personal Information Protection Act and, by extension, the Maryland Consumer Protection Act by engaging in the conduct alleged herein.

203. Independently, Defendant has violated the Maryland Consumer Protection Act by engaging in the unfair and deceptive practices alleged herein. Pursuant to the FTCA, and Maryland law, Defendant was required by law, but failed, to protect Plaintiffs' and the Class's PII and maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' PII. This constitutes a violation of Maryland's Consumer Protection Act.

204. The damages suffered by Plaintiffs and Class Members were directly and proximately caused by the deceptive, misleading, and unfair practices of Defendant, as described above.

205. Plaintiffs and Class Members seek declaratory judgment that Defendant's data security practices were not reasonable or adequate and caused the cyberattack under the Maryland CPA, as well as injunctive relief enjoining the above described wrongful acts and practices of Defendant and requiring Defendant to employ and maintain industry accepted standards for data management and security, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

206. Additionally, Plaintiffs and Class Members make claims for actual damages, attorneys' fees, and costs.

SEVENTH COUNT
Violation of the Maryland Personal Information Protection Act.
Md. Comm. Code §§ 14-3501, *et seq*.
(On Behalf of Plaintiffs and the Class)

207. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

208. The Maryland Personal Information Protection Act requires that "[t]o protect personal information from unauthorized access, use, modification, or disclosure, a business that owns, maintains, or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned, maintained, or licensed and the nature and size of the business and its operations." Md. Code Ann., Com. Law § 14-3503(a).

209. The PII exposed by Defendant's Data Breach qualifies as "[p]ersonal information" under the statute insofar as the PII exposed includes names, Social Security

numbers, passport numbers, government ID numbers, and driver's license numbers. *Id*. § 14-3501(e)(1)(i).

210. The Maryland Personal Information Protection applies to Defendant insofar as Defendant constitutes a "Business." *Id*. § 14-3501(b)(1–2).

211. The Maryland Personal Information Protection applies to Plaintiffs and the Class as they are "individuals" and "customers." *Id*. §§ 14-3502(a) and 14-3503.

212. Defendant violated § 14-3502 insofar as Defendant failed to properly destroy Plaintiffs and Class members information. For example, Plaintiffs graduated years ago—and yet, Defendant continued to unnecessarily maintain Plaintiffs' information in an insufficiently secure manner.

213. As detailed *supra*, Defendant failed to "implement and maintain reasonable security procedures and practices" as to protect Plaintiffs' and Class members' PII from "unauthorized access, use, modification, or disclosure"—this constitutes a violation of § 14-3503(a).

214. Defendant's Data Breach was a "breach of the security system" insofar as the Data Breach was "the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business." *Id*. § 14-3504(a)(1).

215. Moreover, Defendant violated the statute by failing to timely notify Plaintiffs and the Class of the Data Breach—in particular, by failing to adhere to the 45-day notification window to consumers. *Id*. § 14-3504.

216. Defendant's violations of Maryland Personal Information Protection Act also constitute violations of the Maryland Consumer Protection Act, Md. Comm. Code §§ 13-301,

et seq.—and thus trigger that statute's penalty provisions. *Id*. § 14-3508.

217. As a direct and proximate result of Defendant's violations of the Maryland Personal Information Protection Act, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

218. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the dark web.

219. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law.

EIGHTH COUNT
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

220. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

221. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

222. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

223. Given its authority under the Declaratory Judgment Act, this Court should enter a

judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class members.

224. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

225. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

226. And if a second breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs and Class members' injuries.

227. If an injunction is not issued, the resulting hardship to Plaintiffs and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

228. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiffs, Class members, and the public at large.

PRAYER FOR RELIEF

Plaintiffs and Class members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further unfair and deceptive practices;

E. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Dated March 4, 2024 Respectfully submitted,

By: */s/ Courtney L. Weiner*
Courtney L. Weiner (D. Md. #19463)
LAW OFFICE OF COURTNEY WEINER LLC
1629 K Street, NW, Suite 300
Washington, DC 20006
T: (202) 827-9980
cw@courtneyweinerlaw.com

LAUKAITIS LAW LLC
Kevin Laukaitis*
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Raina C. Borrelli*
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703-3515
Telephone: (608) 237-1775
Facsimile: (608) 509 4423
raina@turkestrauss.com

Zachary E. Howerton (D Md. Bar No. 20688)
Roy L. Mason (00922)
SMOUSE & MASON, LLC
223 Duke of Gloucester Street
Annapolis, MD 21401
Telephone: (410) 269-6620
Facsimile: (410) 269-1235
zeh@smouseandmason.com
rlm@smouseandmason.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
5335 Wisconsin Avenue NW
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Counsel For Plaintiffs and
The Proposed Class

**Pro Hac Vice* applications forthcoming

CERTIFICATE OF SERVICE

I certify that on this 4th day of March, 2024, I caused the foregoing to be served via CM/ECF on all counsel of record.

/s/ Courtney L. Weiner